# ERISA ADVISORY COUNCIL

August 24, 2016

# Cyber Risk Management and Insurance

Eric C. Nordman, CPCU, CIE, Director

Regulatory Service Division & the CIPR

NAIC

National Association of Insurance Commissioners

& The Center for Insurance Policy and Research

# Agenda

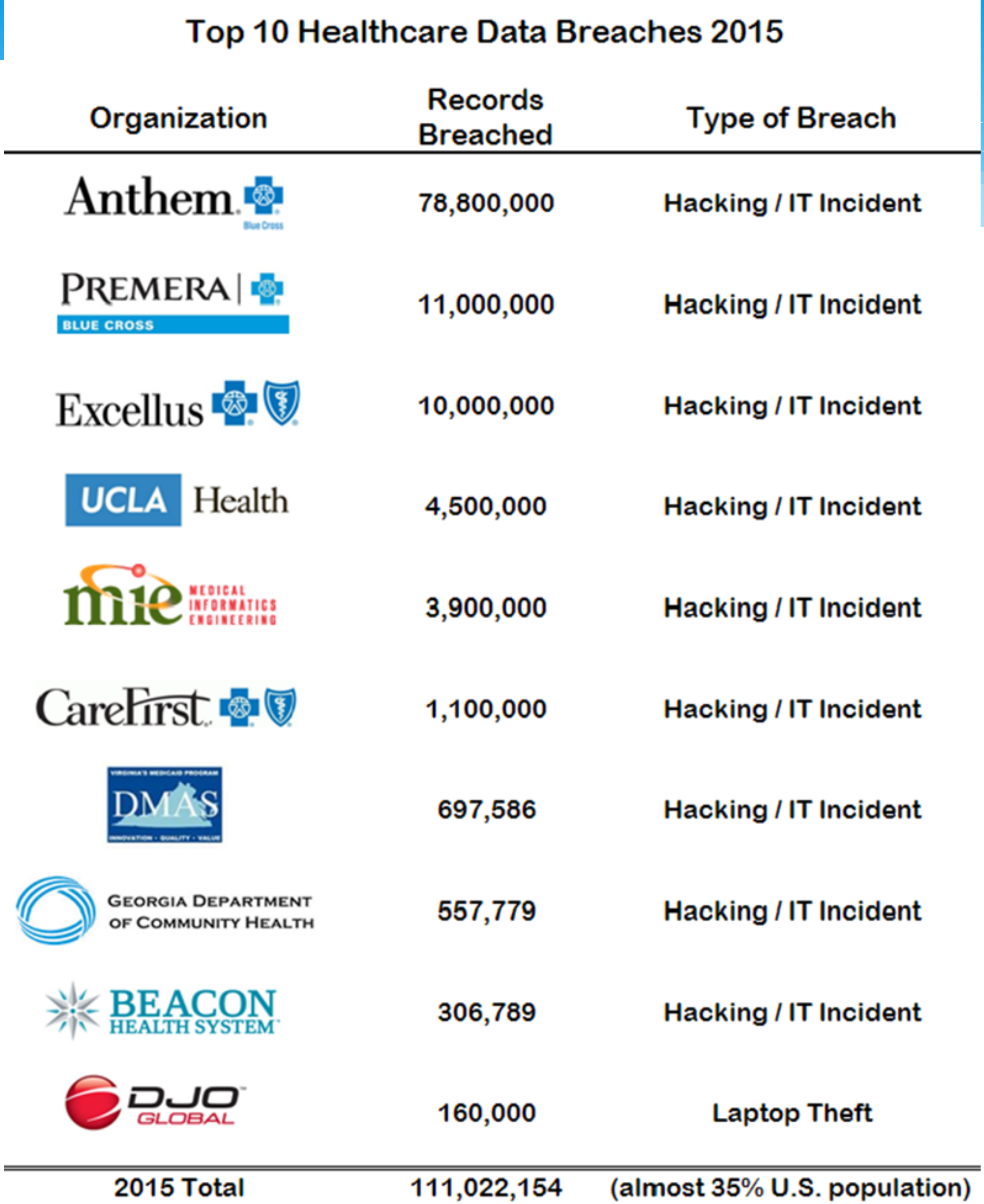
- Managing Cyber Risks
- Classifying Cyber Threats
- What Consumers Expect from Businesses
- Managing Business Risks
  - Sound Cybersecurity Hygiene
  - Cybersecurity Insurance Policies
- Underwriting Cybersecurity Insurance
- Unique Risks for P&C Insurers
- Information Collected by Regulators

# Managing Basic Cyber Risks

- Study by IBM & the Ponemon Institute
- $7.01 million is the average total cost of data breach
- $221 is the average cost per lost or stolen record
- The biggest financial consequence is lost business
- The longer it takes to detect the more costly it is to resolve
- Regulated industries have the most costly data breaches
  - Fines and the higher than average rate of lost business
  - Healthcare and financial services

# Managing Basic Cyber Risks

| Per Capita Cost by Industry Class | of Benchmarked Companies (Ponemon) |
|---|---|
| Health | $402 |
| Financial | $264 |
| Transportation | $247 |
| Education | $220 |
| Retail | $200 |
| Media | $177 |
| Hospitality | $148 |



## Top 10 Healthcare Data Breaches 2015

| Organization | Records Breached | Type of Breach |
|---|---|---|
| Anthem. Blue Cross | 78,800,000 | Hacking / IT Incident |
| PREMERA BLUE CROSS | 11,000,000 | Hacking / IT Incident |
| Excellus | 10,000,000 | Hacking / IT Incident |
| UCLA Health | 4,500,000 | Hacking / IT Incident |
| mie MEDICAL INFORMATICS ENGINEERING | 3,900,000 | Hacking / IT Incident |
| CareFirst | 1,100,000 | Hacking / IT Incident |
| DMAS | 697,586 | Hacking / IT Incident |
| GEORGIA DEPARTMENT OF COMMUNITY HEALTH | 557,779 | Hacking / IT Incident |
| BEACON HEALTH SYSTEM | 306,789 | Hacking / IT Incident |
| DJO GLOBAL | 160,000 | Laptop Theft |
| 2015 Total | 111,022,154 | (almost 35% U.S. population) |

# Classifying Cyber Threats

- Common Cyber Risks
  - Identity Theft
  - Business Interruption
  - Reputational Damage
  - Damage or Theft of Valuable Assets
  - Malware
  - Human Error
  - Cost of Credit Monitoring Services
  - Trademark or Copyright Infringement

# Classifying Cyber Threats

- Identity Theft:
  - Unauthorized use or attempted use of an existing account
  - Use of personal information to open a new account
  - Misuse of personal information for a fraudulent purpose
- Malicious Software (Malware):
  - Trojans
  - Worms
  - Viruses
  - Botnet

# Classifying Cyber Threats

- Cyber Crime Perpetrators
  - Nation States
  - Organized criminals
  - Lone wolf criminals
  - Hacktivists
  - Hobbyist for fun or practice

# Consumer Expectations

- Consumers expect business/government will:
  - Protect the information they provide
  - Provide information on what is collected
  - Tell them who has access to their information
  - Provide access to your privacy policy
  - Receive notification if there is a breach
  - Be informed about remediation efforts
  - Be provided assistance with steps to take to protect themselves from identity theft or fraud

# Managing Business Risks

- Sound cybersecurity hygiene
- Develop a sound cybersecurity framework
  - Identify
  - Protect
  - Detect
  - Respond
  - Recover

# Managing Business Risks

- Identify
  - Know what personally identifiable information (PII) you collect and why
  - Assess threats to the information you maintain
  - Understand how PII can be accessed
  - Develop a written plan of action and practice it

# Managing Business Risks

- Protect
  - Limit network access as much as possible
  - Build in redundancy to systems
  - Implement strong user name and password controls
  - Update software frequently (automated updates when possible)
  - Encrypt data whenever possible
  - Train your employees
  - Consider purchase of cybersecurity insurance

# Managing Business Risks

- Detect
  - Monitor networks for threats
  - Look for anomalies or unauthorized users
  - Understand impact of a potential threat
  - Consider joining an information sharing and analysis center

# Managing Business Risks

- Respond
  - Implement your cybersecurity plan
  - Contain the threat and deny access to the bad actor
  - Notify appropriate law enforcement and regulatory authorities
  - Notify impacted consumers and offer remediation assistance

# Managing Business Risks

- Recover
  - Restore data systems and data
  - Help impacted consumers
  - Update your response plan from lessons learned in its execution
  - Train your employees on lessons learned

# Underwriting Cyber Insurance

- The origin of cybersecurity insurance:
  - Errors & Omissions (E&O) coverage
    - Professional liability coverage for businesses
    - E&O for tech companies covered network crashes,  data breach, loss or destruction of data and similar events

# Underwriting Cyber Insurance

- Cybersecurity as a separate peril
  - May 2014: The first cyber exclusion appears in an Insurance Services Office, Inc. Commercial General Liability policy form
    - No coverage for “[a]ny access to or disclosure of any person's or organization's confidential or personal information, including patents, trade secrets, processing methods, customer lists, financial information, credit card information, health information or any other type of nonpublic information.”
  - Exclusion applies to both Coverage A (bodily injury) and Coverage B (personal and advertising injury)

# Underwriting Cyber Insurance

- Overview of cyber insurance coverages in the U.S.
  - Liability for security or privacy breaches
  - Costs associated with a privacy breach
  - Costs associated with restoring business assets
  - Business interruption and extra expense
  - Liability associated with libel, slander or copyright infringement
  - Expenses related to cyber extortion or terrorism
  - Coverage for expenses related to regulatory compliance

# Underwriting Cyber Insurance

## First Party Losses

- Data Breach Expenses
  - Cost of forensic investigation
  - Cost of legal advice to determine notice and remediation requirements
  - Cost of notice and remediation, such as credit monitoring or credit freezes
  - Cost of public relations services
- Data Restoration or Replacement
- Business Interruption losses
- Extortion payments
- Losses from Fraud or Theft

# Underwriting Cyber Insurance

## Third Party Losses

- Privacy Liability (liability to consumers affected by data breach)
- Network Security Liability (damage from your network's failure to protect customer information or intellectual property of others)
- Technology Services Liability (damages from your failure in delivering technology services)
- Media Liability/Content Liability (claims for copyright/trademark infringement or defamation)
- Social Media Liability (claims based on statements or disclosures made in social media)

# Underwriting Cyber Insurance

- Other considerations when purchasing a cybersecurity insurance policy
  - Expert assistance to review your security program
  - Expert assistance in evaluation of an attack
    - Threat actor identification
    - Identification and assistance evaluating state notification and remediation laws
  - Expert assistance in managing consumer notice and remediation efforts

# Underwriting Cyber Insurance

- Importance of Risk Management
  - Insurers will evaluate the adequacy of the businesses’ cyber risk management
  - Evaluation of the disaster response plan
    - Networks
    - Website
    - Physical assets
    - Intellectual property
  - Employees access data systems
  - Antivirus and anti-malware software
  - Frequency of system and software updates
  - Performance of firewalls

# Underwriting Cyber Insurance

- Other ways to cover cyber risk exposure
  - Financial Institutions Bonds
  - Commercial Crime Coverage
  - Errors and Omissions (E&O) Coverage
  - Directors and Officers (D&O) Coverage

# Unique Risks for P&C Insurers

- Property and casualty insurers face two distinct cybersecurity risks
  - Ordinary business risks
  - Added financial exposure from offering cybersecurity insurance and risk management products

# Info. Collected by Regulators

- Cybersecurity and Identify Theft Insurance Coverage Supplement
- Information filed April 1 each year
- First data collection April 1, 2016 for 2015 data year
- Initial results:
  - Roughly $500 M Stand-Alone Policies
  - Approximately $1 B in Package Policy Premiums

# Info. Collected by Regulators

- Stand-Alone Cybersecurity Insurance Policies
  - Number of claims reported
  - Direct premiums written and earned
  - Direct losses paid and incurred
  - Adjusting and other expenses
  - Defense and cost containment expenses
  - Number of policies in-force
- Similar info. collected for Identity Theft Insurance

# Resources

- NAIC Cybersecurity Task Force (http://www.naic.org/committees_ex_cybersecurity_tf.htm)
- NIST Cybersecurity Framework (http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf)
- National Conference of State Legislatures has a listing of state data breach and notification laws (http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx)
- SIFMA Small Firm Cyber Guidance & Checklist (http://www.sifma.org/issues/operations-and-technology/cybersecurity/guidance-for-small-firms/)

# Thank You

It’s time for your questions

Eric Nordman
816-783-8005
enordman@naic.org

NAIC
National Association *of* Insurance Commissioners

& *The* CENTER *for* INSURANCE POLICY *and* RESEARCH